A CRITIQUE OF THE EFFECTIVENESS OF CYBER LAWS IN ADDRESSING CYBER HARASSMENT: A CASE FOR UGANDA

MARIAM MIREMBE

CKS21B11/026

A DISSERTATION SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF UGANDA CHRISTIAN UNIVERSITY

May,2025

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, Mirembe Mariam, solemnly declare that I solely and on my initiative conducted this research and swear to the best of my knowledge that the research was conducted based on the standard ethics and thus no plagiarism or computer misuse was carried out.

Signature: 

Date: 26th, May, 2025

APPROVAL

This dissertation has been prepared under my close supervision and guidance as the university supervisor.

Signature: 

Mr. Daniel Kisa

Date: 26th, May, 2025

ACKNOWLEDGEMENT

I, Mirembe Mariam, do hereby acknowledge the following research study was conducted solely by me using the various sources of information without plagiarizing anyone's work. This research was completed with guidance and support from my supervisor Mr. Kisa Daniel who did his best to provide me with wisdom and knowledge about how to conduct my research so as to come up with meaningful research. In addition to my supervisor, I would like to acknowledge the support from my dear parents and my colleagues who kept on encouraging me and providing me with the required materials for my research.

TABLE OF CONTENTS

ABSTRACT

Cyber harassment is the use of a computer for making any requests, suggestions or proposals which is obscene, lewd, lascivious or indecent, threatening to inflict injury or physical harm to the person or property of any person. Cyber harassment is a growing evil that has been taking place since the invention of computer chat rooms to the creation of Facebook, twitter, tiktok, among others. With the presence of these various communication forums and the ability of users to remain anonymous, cyber harassment has become a daily crime, causing its victims to suffer from depression, self-denial, isolation and sometimes suicidal thoughts. This research basically looks at the effectiveness of cyber laws such as the Computer Misuse Act Cap 96, Access to Information Act Cap 95, and Data Protection and Privacy Act Cap 97, in curbing cyber harassment. The research shall be table-based (qualitative), specifically based on the available literature on the research topic as well as the required statutes, and it shall focus on the general population as the victim to cyber harassment. This research is expected to amplify the voice in the fight against cyber harassment as well as provide new measures to help curb the evil.

CHAPTER ONE

1.0 INTRODUCTION

The evolution and invention of information and communication technology (ICT) over the past years have altered the social environment and have in many ways directed society's interactions. As of today, many people, especially the youth, have led in the daily usage of ICT tools such as mobile phones, computers, among others. Although these ICT tools are beneficial, they have inadvertently opened up new avenues for cybercrimes, such as cyber harassment

Cybercrime is any criminal activity involving a computer as the target or tool of the crime[1]. Cyber harassment is a form a cybercrime whereby one person uses a computer to make any requests, suggestions or proposals which are usually obscene.

lascivious or indecent, threatening to inflict injury or physical harm to the person or property of any person, or knowingly permitting any electronic communications device to be used for any of the above purposes[2].

Cyber harassment is an evil that has been taunting people since the development of technology such as telegraphs in the 1830s and has been going on with the further evolution of technology such as the internet, leaving many victims facing depression, anxiety, psychological distress, social isolation and sometimes suicidal thoughts.

On the brighter side, various states have come up with different laws and regulations

[1] **Oxford Advanced Learner's Dictionary**

[2] Section 24 as quoted from the Computer Misuse Act Cap 96

to curb cyber harassment. In Uganda, the legislature enacted the Access To Information Act cap 95 Computer Misuse Act Cap 96 and the Data Protection And Privacy Act Cap 97 which contains laws criminalizing any form of cybercrime.

1.1 BACKGROUND OF THE STUDY

Cyber harassment started way back in the 1990s during the popularization of affordable computers and the introduction of online forums, chat rooms and social media sites where anonymity led to increased instances of abusive behaviour. This anonymous nature of the Internet provided a fertile ground for online harassment, including trolling and flame wars in forums and chat rooms, especially among teenagers.

The rise of social media platforms such as Facebook, Instagram and Twitter in the early 2000s and of recent Tiktok significantly heightened the rate of cyber harassment, allowing individuals to easily target others with negative comments, rumours, and personal attacks. The other reason why cyber harassment has continued to grow is due to the fact that individuals fail to protect their private information through the use of strong and rare passwords, make social media accounts public, thus allowing everyone to view and also use the information to harass them, lack of strict laws against the vice.

In the mid-2000s, an 18-year-old girl named Jessica Logan killed herself after her boyfriend sent her nude pictures to at least 7 teenage schools in Ohio, thus resulting in her being cyber harassed. [3] In 2007, a 13-year-old Megan Meier committed suicide after some people created a fake MySpace profile under the name Josh Evans to harass her.

[3] https://www.bark.us visited on 21st march 2025

A federal found the perpetrators guilty of conspiracy and unauthorized computer use.[4] Similarly, in 2012, Amanda Michelle Todd committed suicide because of the constant cyber harassment she faced from Internet trolls[5].

In 2023, the LGBTQI community in Ethiopia faced continuous harassment and threats of physical violence with posts being shared on Tiktok some having their names and pictures and hashtags saying whip, stab and kill any transgender or homosexual in Ethiopia.

In an article written in the Makerere University Directorate for ICT Supports[6], **Thierry Henry[8]**, a former Arsenal player stated that 'the sheer volume of mental torture due to racism and bullying of individuals is rampant on the Internet that it has become too toxic to ignore' This statement is a further eye opener to show that cyber harassment still exists on the Internet.

In Uganda, a prominent singer was harassed by releasing her nude pictures which were later posted all over social media platforms. Likewise, Stella Nyanzi was charged with

[4] The case spurred the state of Missouri thereby giving rise to the enactment of the AntiHarassment Act in the state.

[5] http://thecanadianencyclopedia visited on 21st march 2025

[6] Arthur Moses Opio, (2023), report on understanding cyber bullying, Makerere University

Directorate for ICT Supports, Uganda, <http:// dicts.mak.ac.ug visited on 21st March, 2025. [8] Thierry henry is a former football player and legend in the arsenal football team currently working as a football pundit and broadcaster for CBS.

cyber harassment pursuant to section 24 of the Computer Misuse Act for harassing H.E President Yoweri Kaguta Museveni, on her social media accounts [7]

Due to the existence and continued growth of such cases, governments all over the world came up with laws in relation to curbing of cyber harassment.

In Europe, a set of guidelines known as the General Data Protection Regulation (GDPR)[8] was put formulated and its major aim is to ensure that individuals have greater control over their personal data. This is because most of the cases of cyber harassment arise out of one individual getting into contact with another person's information and thereby using such information to harass them.

In Uganda, various laws have been enacted to curb the vie and these include Access To Information Act Cap 95, Computer Misuse Act Cap 96, Data Protection And Privacy Act Cap 97. These laws were put into place to protect individuals and their personal data from unauthorized access to information and also to prescribe punishment for those held liable.

These laws have played a big role to bringing justice to the victims of cyber harassment a case to consider is that of Uganda v Brian Isiko (2020) where Brian Isiko was convicted for harassing the woman MP for Kabarole district by continuously sending her love messages which were considered obscene and rude by the victim.

[7] Stella Nyanzi v Uganda (No.79)(2019)[2020] 1 UGHCCRD www.monitor.co.ug

[8] The GDPR is a European law that is aimed at strengthening individual's data protection rights and regulating the processing of personal data by organizations, both within and outside the European Union.

1.2 STATEMENT OF THE PROBLEM

Cyber harassment is a computer related crime that has continued to exist from the invention of computer chat rooms to the creation of social media platforms. Even with the existence of legislature to curb it, cyber harassment has continued to exist. This attributed to the fact that some of the available laws are ineffective in their applicability or do not address the general aspect of the crime but rather a portion of it, some people are ignorant of the existence of such laws and therefore there is need teach the mass about the laws, the laws are not strict enough to deter an offender from committing the crime and the fact that anonymity is guaranteed makes it easy for the perpetrators to harass their victims without fear. This research is therefore made to provide solutions to these factors that are still keeping the vice of cyber harassment in existence.

1.3 OBJECTIVES OF THE STUDY

1.3.1 GENERAL OBJECTIVES

To ascertain the effectiveness of cyber laws in resolving the vice of cyber harassment.

To identify the challenges that hinders the effectiveness of cyber laws in curbing cyber harassment.

1.3.2 SPECIFIC OBJECTIVES

To analyze the role of the court in curbing cyber harassment

1.4 RESEARCH QUESTIONS

a) What challenges hinder the effectiveness of cyber laws in curbing cyber harassment?
b) What is the role of the court in curbing cyber harassment?
c) How have the available cyber laws been used to resolve the vice of cyber harassment?

1.5 SIGNIFICANCE OF THE STUDY

The purpose of the research is to build on the existing knowledge about the ways of curbing the evil of cyber harassment. Though various laws have been put in place to curb cyber harassment, such as **Section4**[9] Cap 96 and **Section 7**[10], the vice has continued to exist and therefore the purpose of this research is to amplify the already existing laws and regulations put in place to curb the vice by sensitizing and educating the masses about the law.

To introduce new ideas that should be adopted such as making much more strict laws to punish offenders, internet providers making restrictions on what should be posted, sensitizing the masses on the dangers of cyber harassment both to the victims and the harassers and emphasizing strict privacy through use of strong and different passwords for every social media platforms.

To revise the existing laws by removing that which is no longer necessary and

applicable to the society and input laws that are applicable to the society.

[9] Computer Misuse Act Cap 96

[10] Data Protection and Privacy Act Cap 97

1.6 SCOPE OF THE STUDY

The scope of the study shall encompass the temporal/time scope, geographical scope, as well as the thematic or subject/scope in relation to the study problem.

1.6.1 TEMPORAL SCOPE

The research took a short time frame, specifically aiming at the period of time since the law against cyber harassment was implemented to date. The research also took a short time due to the matter of fact that it is desk-based research or a research based on reviewing and building on the existing data about the study.

1.6.2 GEOGRAPHICAL SCOPE

The research is based mainly on Uganda, though focus is put on the international scene as well as a way of showing that the vice of cyber harassment not only affects Uganda but the whole world as well.

1.6.3 SUBJECT/THEMATIC SCOPE

The research centres on cyber harassment as an internet vice affecting people who fall victim to it.

1.7 LITERATURE REVIEW

The article[11] written in the Makerere University Directorate for ICT Support (**DICTS)** on Sunday 26th March, 2023, talks about some of the aspects of cyber bullying and or cyber harassment. In this article, the author cites **Thierry Henry**, a former Arsenal football

[11] Arthur Moses Opio, (2023), understanding cyber bullying, Makerere university directorate for ICT support (DICTS), Uganda < https://dicts.mak.ac.ug visited on 21st March 2025.

player who stated that it was far easy to create an account on social media and use it to harass and bully others without consequences because of the anonymity. This article also states the fact that research has it that one in three young people in thirty countries have been a victim to cyber bullying thus making many lose self-esteem and some dropping out of school eventually thus stipulating some of the actions that accrue to cyber harassment, however, it brings about neither any legal solutions such as parliamentary laws or regulations set in place to curb the vice for example the Computer Misuse Act and Data Protection and Privacy Act which were implemented to regulate the use of computers especially the internet and also to regulate the access to one's information by another, nor non- legal solutions to help resolve and curb cyber harassment such as educating the masses about the need to protect their data using uncommon and different passwords, keeping their accounts private and deleting all digital footprints, that are most important in the fight against cyber harassment.

Another article in relation to the research topic is that from the **World Health Organization**[12] written in 27th March,2024 talking about the fact that the rate of cyber bullying or harassment in school- going children has increased from 12% -15%in boys and from 13%-16% in girls. The article continues to state that though the digital world offers the young people a learning environment as well as a cast opportunity for connections, it also amplifies challenges like cyber harassment. It is therefore crucial for the government, families and schools to collaborate and come up with comprehensive

[12] World Health Organization, (2024), **one in six school-aged children experience cyber bullying,** WHO/Europe, Copenhagen Denmark <https://www.who.int, visited on 21st march 2025.

strategies to handle online risks such as cyber harassment. In addition to what this article states, I will suggest that the internet time for the young people be regulated as well as setting parental guidance rules on what is accessible to the children as well as ensuring that communications between the children and any other person is monitored. By doing so, the levels of cyber harassment in young people shall surely decrease.

The case **Stella Nyanzi v Uganda** [13]clearly sets out what entails cyber harassment. In this case Stella Nyanzi harassed President Yoweri Kaguta Museveni and also criticized the first lady Janet Kataha Museveni for not providing sanitary pads to students at school, on her social media platform. Court stated that anything done or said by one person with the aim of ruining the reputation of that person makes such a person liable for cyber harassment. Therefore, in this case, court upheld the law under Section 24 of the Computer Misuse Act Cap 96. Though Stella Nyanzi insisted that she had the right to freedom of speech, court upheld the fact that no person shall enjoy a right while inflicting the rights of another. This case shows that the courts of law have upheld the laws in regards to curbing cyber harassment.

Another similar case is that of **Uganda v Brian Isiko**[14] where Brian Isiko continuously sent love messages to the then woman member of parliament for Kabarole district which messages were interpreted by the victim as obscene and rude. Court upheld the law in regards to cyber harassment and the perpetrator was duly convicted. This case

[13] *Op.Cit*

[14] ibid

laid a precedent to all cases in relation to cyber harassment in Uganda today.

CHAPTER TWO

2.0 RESEARCH METHODOLOGY

2.1 INTRODUCTION

The research methodology includes the research design, sampling techniques and limitation of the study. The study is generally based on the qualitative approach. This is because the qualitative approach aims at gathering and analyzing non-numerical data to gain insight or in-depth exploration into people's experiences, perceptions and behavior in regards to cyber harassment and how the laws of Uganda have managed to and also failed to handle the vice with specific emphasis put on the Computer Misuse Act Cap 96 and the Access To Information Act Cap 95. This research reviews the existing legal frameworks with emphasis on Uganda's legal fraternity. The research also reviews the existing works of the several scholars, in relation to cyber harassment

The research is also based on the desk research methodology. The desk research methodology provides a comprehensive exploration of the research report from the existing resources mainly from the Computer Misuse Act Cap 96, Access To Information Act Cap 95, Data Protection And Privacy Act Cap 97 as well the constitution of the republic of Uganda, 1995 as amended, case law, articles, reports and other legal documents in relation to the research topic.

Data for the research was also obtained from reliable online libraries, articles, journals, e-books and websites that encompass various ideas and suggestions from different authors and publishers which guided and directed the research.

2.2 RESEARCH DESIGN

The study adopts a qualitative research design which ascertains the effectiveness of cyber laws in curbing cyber harassment. The study adopts a case study and context analysis approach to examine the existing laws and their enforcement as a way of curbing cyber harassment.

A qualitative research design is the best approach for this study because it employs an in-depth exploration of the legal and social dynamics surrounding cyber harassment such the works of the different scholars, the available statutes, legal reports and information from the victims giving it a more sense of reality.

2.3 SAMPLE SIZE AND SAMPLING TECHNIQUE

The sample size shall consist majorly consist of five groups of people, that is, the legislature, law enforcement bodies such as courts, information technology professionals as well as any experienced members of the public.

The study shall base on the purposive sampling technique to target the specific participants with the relevant information/ knowledge and experience in regards to cyber harassment and how to enforce policies to curb the vice. The purposive sampling technique ensures that only specific individuals with knowledge and in-depth about the study topic are included in the study.

2.4 STUDY POPULATION

The study population shall consist of stakeholders involved in enforcement of policies against cyber harassment. This shall include policy makers, law enforcement bodies, regulatory authorities such as the National Information Technology Authority – Uganda (NITA-U), legal experts and organizations advocating for the fight against cyber harassment. This target population is chosen based on their expertise and involvement in the enforcement of laws against cyber harassment

2.5 LIMITATIONS OF THE STUDY

These are some of the constraints that may affect the results or interpretation of the findings of the study. The limitations of the study include among others, methodological limitations, time constraints, scope of the study, access to data and research bias.

2.5.1 METHODOLOGICAL LIMITATION

This involves sample size limitation whereby the selected sample size is usually small and may not represent the larger population as well as ineffective data collection methods such as context analysis and case study which may employ the researcher's bias as well as influence.

2.5.2 TIME RESRAINTS

Due the presence of a limited time to conduct the research, the depth of the study and the amount of the data collected and analyzed may be limited. This therefore calls for the proper allocation of sufficient time to thoroughly conduct the research to come up with sufficient and useful data

2.5.3 SCOPE OF THE STUDY

The fact being the study majorly focuses on the effectiveness of cyber laws in curbing cyber harassment in Uganda limits the applicability of results from other contexts to the research in the study, thus resulting in producing less information on the research topic compared to when the scope is wider

2.5.4 ACCESS TO DATA

Due to the fact that some of the sources of data in relation to cyber harassment are either incomplete, have restricted access to relevant information, it limits the amount of information input in the study.

2.5.5 RESEARCH BIAS

Most of the times, research includes information which the researcher feel is more important leaving out the rest which would have been essential to build a good research. This clearly indicates research bias and therefore it sometimes hinders the possibility of discovering new data on the study.

2.6 DATA ANALYSIS

The data was analyzed using thematic content analysis since the research employed the qualitative approach. Thematic content analysis involves coding whereby key themes, patterns and ideas within the data are assigned codes or labels and presented in an organized manner. The themes are coded to provide an insight into the

loopholes in the legal framework concerning cyber harassment, the non-legal aspects that give rise to cyber harassment.

2.7 ETHICAL CONSIDERATION

The study strictly adhered to all ethical guidelines and considerations to ensure that there is no form of **plagiarism** by ensuring that all the information from known primary and secondary sources is clearly referenced, no form of **computer misuse** was done during the research as all the information was attained with authorization (no hacking was done) and there was compliance with the university dissertation rules. The research also ensured the privacy of the participants especially those that are victims of cyber harassment whose interactions provided information that was used to build the research.

CHAPTER THREE

3.0 NON-LEGAL FACTORS THAT GIVE RISE TO CYBER HARASSMENT

Though many people fall victim at the hands of cyber harassment due to the inadequacy and ineffectiveness of cyber laws, there are several other non-legal factors and challenges that have continued to guarantee and harbour cyber harassment in Uganda today. This section focuses on the factors beyond the formal legal framework that contribute to or influence cyber harassment in Uganda.

3.1 Socio-cultural Norms

Socio-cultural norms refer to the acceptable beliefs or behavior that society recognizes or follows. These norms curve the ideal nature through which an individual in that society should carry out their duties or actions. For example if the norms stipulate a certain way which women should behave both in society and online, any deviation from these norms renders them vulnerable to cyber harassment. Usually, if there is any deviation from the norms by the victim and she is harassed, society perceives it in a way that she brought it upon herself and will be blamed instead of the harasser, hence making it difficult to fight cyber harassment.

Norms also determine what should be considered private and what is public for disclosure. It should be noted that norms vary widely across cultures, in that what is considered acceptable for sharing personal details in one culture, another culture might consider it highly inappropriate. Therefore, the lack of uniformity in views makes it very challenging to establish a universal law for cyber harassment as well as to enforce it across the different cultures of people on different online platforms.

3.2 Digital Literacy

Digital literacy is the ability to use digital technology, communications, tools and networks to locate, evaluate, use and create information. People with higher digital literacy are better equipped to identify and avoid cyber harassment compared to someone with less digital literacy. Digital literacy allows individuals to evaluate online information and recognize manipulative tactics used by online harassers.

However, it should be noted that though digital literacy is a strong tool against cyber harassment, the question remains, how many people are digital literates? Report has it that only 20% of Uganda's population has digital literacy.[15] This therefore means that Uganda's biggest percentage of the population is digital illiterates and therefore prone to cyber harassment.

3.3 Digital Awareness

Digital awareness refers to the understanding of the risks and consequences of online behaviour as well as the impact of digital technologies on society. It should be noted that digital awareness encourages responsible online behaviour because people understand the potential harm of their actions, hence desisting from harassing others or uploading risky information. Digitally aware people are more likely to recognise cyber harassment compared to those who aren't digitally aware.

Most of the people who are victims of cyber harassment are people who lack digital awareness. Therefore, in order for cyber harassment to be wiped out, the public has to be sensitised about digital awareness to prevent the risks that come with a lack of it.

[15] Talent Atwine Muvunyi, 2025, News Report Reveals Uganda's 5 Most Digitized And Highest Paying Jobs, Uganda, www.c-news.ug ,visited on 13th may 2025.

3.4 Community and Peer Influence

Community and peer influence play a big role in the reason why some people act in particular ways. Most people carry out activities because of the hype they receive from their peers and the community that makes them believe whatever they are doing is the best to the extent that some upload videos of their nudes, engage in unethical activities that degrade them in the society; which make them prone to cyber harassment in case such information is came across by the harassers.

This therefore makes it difficult to enforce cyber harassment regulations in such communities and on such people, hence giving a foothold to cyber harassment.

3.5 Permissiveness On Some Social Media Platforms

With the evolution of computers and the invention of internet, the online community has grown rapidly grown with the presence of various media platform. These include **Facebook, Instagram**, **Tiktok**, **X**, **Whatsapp** and many others. Al these platforms set different sets of laws that govern its use and bleach of the rules could either result in the banning of the users account or blacklisting and confiscating such information before it is exposed to the general public for consumption.

Some actions that constitute cyber harassment are easily carried out on some social media platforms due to the fact that these social media platforms put no restrictions to the information share by the people on the platform.

Whereas some platforms have put up rules that govern the nature of information posted by people as well as giving penalties to those that abuse or go against the rules, some platforms have continued to be permissive that encouraging the vice of cyber

harassment to continue existing on the online community hence making it difficult to curb the vice.

Lack of parental guidance.

Many children are being cyber harassed due to a lack of parental guidance on what information they should share with the online community, as well as what information they ought not access. Due to the presence of freedom, children often fall into the snares of cyber harassers who use the information they share online to harass them.

Individuals, parents, communities and the government should therefore look for various ways to ensure that the above-mentioned aspects are resolved, as the only way cyber harassment can be curbed.

As the African adage says, **'if you want to get rid of the weeds in the garden, do not slash them but rather uproot them to prevent regrowth of the same'**

CHAPTER FOUR

4.0 ROLE OF COURT IN CURBING CYBER HARASSMENT

Courts have indeed played an important role in curbing cyber harassment, although it is just an evolving area of the law.

4.1 Establishing Legal Precedents

Courts have established legal precedents which act as roadmaps for future cases. When court rules on a cyber-harassment case, the ruling in such a case can influence how such similar cases are to be handled in the future. An example of a precedent for cyber harassment is the case of **Uganda V Brian Isiko**[16] a case that gave meaning to cyber harassment as well as a prudent foundation for cases regarding cyber harassment.

4.2 Establishing Civil Lawsuits For Damages

Courts have set a fertile ground for victims to sue harassers in civil courts to seek compensation for damages such as emotional distress and reputational harm. Once a victim of cyber harassment sues the harasser and is successful, the harasser is bound to pay damages prayed for by the victim as well as those that the court may deem fit.

4.3 Criminalizing Cyber Harassment

Courts have also gone ahead to interpret and apply criminal laws relating to cyber harassment, which can later result in criminal charges and penalties for the harasser. For example, the case of **Uganda V Brian Isiko**[17] was handled in the High Court Criminal Division, meaning that it was treated as a criminal case. This serves as a limiting force to those intending to carry out cyber harassment, thus reducing its growth.

[16] Uganda v Brian Isiko(No. 0084) [2018] HCCD
[17] ibid

4.4 Issuing Of Protective Orders

Once a victim to cyber harassment sues a harasser, court usually issues protective orders also known as restraining orders to prevent further harassment.

It should be noted that the restraining orders restrict any contact between the harasser and the victim.

CHAPTER FIVE

5.0 5.0. LEGAL ASPECTS GOVERNING CYBER HARASSMENT

Uganda as a state has come with laws to resolve the vice of cyber harassment and these include the **Computer Misuse Act Cap 96** and **Data Protection And Privacy Act**

5.1 Cap 97

The Computer Misuse Act cap 96, under section 24 provides for both the definition and penalty for cyber harassment. It provides that;

- Cyber harassment is the use of a computer for making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent, threatening to inflict injury or physical harm to the person or property of any person or knowingly permitting any electronic communications device to be used for any of the above purposes.
- The act provides that any person who commits cyber harassment is liable on conviction to a fine not exceeding seventy-two currency points or imprisonment not exceeding three years, or both.

This law is a great backbone in the fight against cyber harassment, and it has brought justice to many who have fallen victim to cyber harassment.

In the case of **Uganda V Brian Isiko**[18]The perpetrator, Brian Isiko, was charged with cyber harassment contrary to section 24[19] for continuously sending harassing messages to the then Kabarole woman member of parliament. The court sentenced the perpetrator to two years of imprisonment. Hence, giving justice to the victim as well as amplifying the law so that more people are aware of what it fights for.

[18] Uganda v Brian Isiko (No.0084)[2018] HCCD

[19] Computer Misuse Act Cap 96

In the same light, **Stella Nyanzi**[20] was arrested and charged with cyber harassment contrary to section 24 of the Computer Misuse Act Cap 96 after posting degrading statements about the president H.E Yoweri Kaguta Museveni and the first lady Janet Kataha Museveni on her social media platforms.

This also served as an awakening to the many social media users who blatantly post degrading statements against other people hiding in the preface of freedom of expression.

The computer misuse act also provides law against **unauthorized access to information**.[21] It provides that any person who without authorization accesses or intercepts any program or another person's data or information, voice records or video records another person or shares any information about or that relates to another person commits an offence.

Most of the perpetrators of cyber harassment usually hack into their victims' computers to access their personal information while others privately voice record or video record their victims and they later on use that information to blackmail and cyber harass the victims. Fortunately, the law under section 11 of the act criminalizes it and therefore all offenders must be aware of the repercussion of carrying out such an act.

The **Data Protection And Privacy Act** [22] is another statute enacted by the law makers whose major role is to provide for protection of the privacy of the individual and of personal data by regulating the collection and processing of personal information.

[20] Stella Nyanzi is a Ugandan human rights advocate, poet medical anthropologist and scholar of sexuality.

[21] Section 11 of The Computer Misuse Act Cap 96

[22] Cap 97

Section 7(1)[23] provides that a person shall not collect or process personal data without the prior consent of the data subject.[24] Most of the victims of cyber harassment face the peril because of the unauthorized access to their personal information by their harassers.

Section 9(1)[25] provides that a person shall not collect or process personal data which relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, and health status or medical records of an individual.

Most of the time, cyber harassers use the above-mentioned information to harass their victims and to force them into doing what they want, which later results in damage to the victim's reputation, depression and sometimes suicidal thoughts because such information is personal.

As explained above, the laws in regards to cyber harassment have played a big role in reducing the occurrence of the vice due to the fact that it is clearly defined to show what constitutes cyber harassment and the related offences, plus the penalty associated with the offence.

However, though these rules have been enacted and implemented, to a greater extent, many perpetrators are on the loose because it is a bit complicated to sue someone based on cyber harassment due to the lack of a set form of evidence needed to charge someone with the offence of cyber harassment and also the fact that some members of the public the not aware of the law relating to cyber harassment and therefore they continue

[23] ibid

[24] Section 2 (ibid) defines data subject to mean an individual from whom or in respect of who personal information has been requested, collected, collated, processed or stored.

[25] Data Protection and Privacy Act cap 97

suffering without any help, hence the need for sensitization and educating people about the laws.

CHAPTER SIX

6.0 SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSIONS

6.1 INTRODUCTION

This chapter rounds up what the research is all about giving a summary of what was intended to be put across, as well as the recommendations and suggestions that the researcher wants to put across as a way of resolving the vice of cyber harassment.

6.2 SUMMARY OF FINDINGS

The vice of cyber harassment has existed since the evolution of computers, especially the internet. Therefore, lawmakers came up with and continue enacting laws to curb the vice.

All over the world, various states have come up with laws to fight the vice in their countries as well as treaties and conventions to ensure that no person in any country that is a signatory to the treaty or convention suffers the vice of cyber harassment without legal aid. An example of the conventions is the **UN Convention on Cybercrime of 2024,** which prohibits the unauthorised access to information systems, including illegal interception of electronic data.

In Uganda today the law has been put in place to curb cyber harassment. Article 27(2)[26] provides that no person shall be subjected to interference with the privacy of that person's .., communication or other property. By providing for privacy, the law ensures that individuals are protected from unauthorized access to their personal information which would be used by the harassers against such an individual.

[26] Constitution of the republic of Uganda 1995 as amended

The **Computer Misuse Act Cap 96** provides for cyber harassment[27]giving a definition to what constitutes cyber harassment as well as laying down the penalty for committing the offence of cyber harassment. This was given more insight in the case of **Uganda V Brian Isiko.**

The **Data Protection and Privacy Act Cap 97** also provides for the law regarding to unauthorized access to information[28] which provides that one ought to get consent from the data subject before processing or collecting the data failure of which results into commission of an offence.

With the presence of this law, individuals are guaranteed of the protection of their information and less attacks from cyber bullies due to the fact that all their personal information is safe.

However, even though these laws have been put in place, the rate at which the vice of cyber harassment is increasing due to majorly some non-legal aspects breeding a fertile ground for the growth of the vice.

The non-legal aspects include peer pressure whereby some of the victims carry out the activities because they are influenced by their peers or community, digital illiteracy whereby some individuals are easily cyber harassed because of their lack of knowledge in regards to what entails cyber harassment, lack awareness as to how to avoid falling victim to cyber harassment and lack of a uniform existent regulations governing the use of computers, the internet and social media platforms.

6.3 RECOMMENDATIONS

[27] Section 24

[28] Section 7(1)

In regard to cyber harassment, the following recommendations ought to be considered;

Sensitization of the public about the law in regards to cyber harassment. It should be noted that many people are suffering at the hands of cyber harassment due to lack of knowledge about the existing laws prohibiting cyber harassment.

Amending the Computer Misuse Act to include a layout of the evidence necessary to charge an individual with cyber harassment so as not to contradict with right to freedom of expression under article 29.[29]

Putting restrictions to what information should be shared on a platform. Social media platform handlers should ensure that regulations regarding what should be shared are enacted and implemented with penalties for failure to follow the regulations.

People should ensure that their personal information is safe by **inserting different and untraceable passwords** on each of their social media platforms. This makes it difficult to easily attain such personal information with the consent of the owner.

Parents should **supervise** their children's time online as well as **insert parental guidance** in their computers to control what information they can access as well as that which they can share.

Government should provide free **platforms for digital literacy** so that people acquire digital knowledge about the use of computers. This is because digital illiteracy has made many people to fall unto the traps of cyber harassers thereby causing havoc for themselves.

[29] Constitution of the republic of Uganda 19995 as amended.

Setting up more strict penalties for cyber harassment. This will demoralize those intending to commit the offence of cyber harassment.

6.4 CONCLUSION

In conclusion therefore, though the law has been put into place to curb the vice of cyber harassment, more work should be done by both the individuals, communities and government to totally erase the vice of cyber harassment.

BIBLIOGRAPHY

JOURNALS/ARTICLES REFERRED TO

Report on understanding cyberbullying by Arthur Moses Opio, Makerere

University Directorate Of ICT

Report by the World Health Organisation about the rise in the cases of children cyberbullied

STATUTES REFERRED TO

Constitution of the Republic of Uganda 1995 as amended

Computer Misuse Act Cap 97

Data Protection And Privacy Act Cap 97

CASE LAW

Uganda v Brian Isiko (No 0088)[2018] HCCD

Uganda v Stella Nyanzi (no. 97)(2019)[2020]

WEBLINKS

https://www.bark.us/

https://thecanadianencyclopedia

https://dicts.mak.ac.ug

https://www.monitor.co.ug/

https://www.who.int

https://www.c-news.ug/